IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

VALERIE ANDERSON, DANIELLE ADAMS, THERESA BREWERTON, JOSEPH CARDENAS, LINDA CAUDILL, CHASSIDY HOLLAND, MARIANA SANCHEZ LOPEZ, JENNIFER MARINO, MELISSA MORALES, TARA HARTZEL VANCOSKY, AND MUHAMMAD ZAHID, individually and on behalf all others similarly situated, Plaintiffs, v. FORTRA LLC, Defendant.	**CASE NO. 0:23-cv-533 (SRN/DTS)** **CONSOLIDATED CLASS ACTION COMPLAINT**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Valerie Anderson, Danielle Adams, Theresa Brewerton, Joseph Cardenas, Linda Caudill, Chassidy Holland, Mariana Sanchez Lopez, Jennifer Marino, Melissa Morales, Tara Hartzel Vancosky, and Muhammad Zahid (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant Fortra LLC ("Defendant" or "Fortra"), a Minnesota corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their

own actions, the investigation of their counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of Fortra's failure to properly secure, safeguard, and adequately destroy Plaintiffs' and Class Members' personally identifiable information ("PII") that it had acquired for its business purposes.

2. Defendant's data security failures allowed a targeted cyberattack in January 2023 to compromise Defendant's network and applications, allowing the hackers to gain access to the information of 130 of Fortra's customers and, as a result, gain access to millions of Plaintiffs' and Class Members' PII (the "Data Breach"). The stolen data includes Plaintiffs' and Class Members' names and Social Security numbers.[1]

3. Defendant is a Minnesota based company that provides information technology management software and services. The Company offers automation, cybersecurity, monitoring solutions, product training, implementation, configuration, upgrades, conversion services. Defendant serves customers worldwide.[2]

4. To provide these services, and in the ordinary course of Fortra's business, Defendant gains access to, acquires, possesses, analyzes, and otherwise utilizes personally

---

[1] Data Breach Notifications, Office of the Maine A.G., https://apps.web.maine.gov/online/aeviewer/ME/40/4cfbf86f-8d04-4296-9195-81b874ba939a.shtml (last visited May 16, 2023).

[2] https://www.bloomberg.com/profile/company/6721124Z:US?leadSource=uverify%20wall (last visited Mar. 6, 2023).

identifiable information, including, but not limited to Plaintiffs' and putative Class Members' names and Social Security numbers. (collectively "Private Information").

5. Plaintiffs and Class Members are nationwide consumers who provided their Private Information directly to Fortra's customers, which included financial institutions, and medical institutions, who then shared the Private Information with Defendant during the regular course of business. Plaintiffs and Class Members also include current and former employees who provided their Private Information directly to Defendant as a term of their employment. Plaintiffs and Class Members each reasonably expected their Private Information would remain private and confidential, whether the information was provided indirectly or directly to Defendant.

6. By acquiring and utilizing and benefiting from the Private Information for its business purposes, Defendant owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiffs and Class Members. These duties required Defendant to design and implement adequate data security systems to protect Plaintiffs and Class Members' Private Information in its possession and to keep this information confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

7. Defendant breached these duties by developing unsafe and unprotected remote access tools, and implementing inadequate data security measures and protocols that failed to properly safeguard and protect Plaintiffs' and Class Members' Private Information from a foreseeable cyberattack on its systems. As a result, unauthorized actors

gained access and exfiltrated and stole Plaintiffs' and Class Members' Private Information. Specifically, the Clop ransomware group, or a related group, TA505, used Defendant's deficient, unsecured, and vulnerable managed file transfer tool, GoAnywhere MFT, to gain remote access to over a hundred of Fortra's customers, including millions of individuals' data.[3] The Clop ransomware group then stole documents stored on the compromised GoAnywhere MFT servers, stealing swaths of data over the course of ten days.[4]

8. Currently, the full extent of the accessed and stolen Private Information, the scope of the breach, and the root cause of the Data Breach are all known by and within the exclusive control of Defendant, its agents, counsel, and forensic security vendors at this phase of the litigation.

9. Defendant breached its duties and obligations in one or more of the following ways: (1) designing, implementing, monitoring, and maintaining unreasonable and knowingly deficient safeguards against foreseeable threats; (2) designing, implementing, and maintaining unreasonable data retention policies; (3) insufficiently training staff on data security and data retention; (4) implementing security measures that did not comply with industry-standard data security practices; (5) omitting from its statements to Plaintiffs and Class Members information about Defendants' inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) implementing data

[3] https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/ (last visited: May 30, 2023).

[4] *Id.*

security measures that were incapable of recognizing or detecting that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents

10. Moreover, based on the type of sophisticated and targeted criminal activity, the type of Private Information Involved, Defendant's admission that the Private Information was accessed, reports of criminal misuse of Plaintiffs and Class Members' Private Information, reports of Plaintiffs and Class Members Private Information on the Dark Web following the Data Breach, the unauthorized criminal third party was able to successfully target and actually obtain Plaintiffs' and Class Members' Private Information, infiltrate and gain access to Defendant's network and its applications to gain access to Plaintiffs' and the Class Members' Private Information, and exfiltrate Plaintiffs' and Class Members' Private Information, including names and Social Security numbers for the purposes of utilizing or selling the Private Information for use in future fraud and identity theft related offenses.

11. As a result of Defendant's inadequate data security and the Data Breach, Plaintiffs' and Class Members' identities are now at a current, imminent, and ongoing risk of identity theft.

12. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that the Plaintiffs' and Class Members' Private

Information was targeted, accessed, has been misused, and disseminated on the Dark Web.[5] Moreover, there is evidence of actual identity theft and misuse of the data following the Data Breach, further establishing that the hackers successfully obtained Plaintiffs' and the Class's PII. This is in addition to the fact that Plaintiffs' and Class Members' Private Information is currently in the hands of a well-known Russian cyber-gang that uses this information for a variety of nefarious purposes, including extortion.[6]

13. As Defendant instructed, advised, and warned in its post Data Breach Notice Letter, discussed below, Plaintiffs and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs' and Class Members' have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will continue to include into the future: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

14. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred

---

[5] https://techcrunch.com/2023/05/04/millions-patients-data-stolen-fortra/ (last visited: May 30, 2023).

[6] https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-begins-extorting-goanywhere-zero-day-victims/ (last visited: May 30, 2023; *see also infra* Fn. 10.

mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time heeding Defendant's warnings and following its instructions in the Notice Letter; (g) deprivation of value of their Private Information; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

15. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that Defendant collected and maintained. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims on behalf of the Class for Negligence (Count one), Negligence *per se* (Count Two), Declaratory Judgment (Count Three), Violation of California's Business Records Act, Cal. Bus. Code § 1798.80, *et seq*. (Count Four), Violation of California's Unfair Competition Law, Cal. Bus. Code § 17200, *et seq*. (Count Five), and Violation of California's Consumer Privacy Act, Cal. Bus. Code § 1798.150 (Count Six).

16. Plaintiffs seek remedies including, but not limited to, damages and injunctive relief, including improvements to Defendant's data security systems and training protocols, future annual audits, and adequate credit monitoring services funded by Defendant,

reasonable attorney fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

18. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and many of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

19. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

PARTIES

20. Plaintiff Valerie Anderson is, and at all times mentioned herein was, an individual citizen of the State of Illinois. Plaintiff Anderson received a Notice Letter via mail dated February 28, 2023 from Hatch Bank notifying her that her Private Information had been impacted during the Fortra Data Breach.

21. Plaintiff Danielle Adams is, and at all times mentioned herein was, an individual citizen residing in the State of Tennessee. Plaintiff Adams received a Notice Letter via mail dated April 21, 2023 from Brightline Medical Associates ("Brightline")

notifying her that her Private Information had been impacted during the Fortra Data Breach.

22. Plaintiff Theresa Brewerton is, and at all times mentioned herein was, an individual citizen residing in the State of North Carolina. Plaintiff Brewerton received a Notice Letter via mail dated April 27, 2023 from NationsBenefits, LLC ("NationsBenefits"), notifying her that her Private Information had been impacted during the Fortra Data Breach.

23. Plaintiff Joseph Cardenas is, and at all times mentioned herein was, an individual citizen residing in the State of Washington. Plaintiff Cardenas received a Notice Letter via mail dated April 7, 2023 from Brightline notifying him that his Private Information had been impacted during the Fortra Data Breach.

24. Plaintiff Linda Caudill is, and at all times mentioned herein was, an individual citizen of the State of Texas, residing in Harris County. Plaintiff Caudill received a Notice Letter via mail dated February 28, 2023 from Hatch Bank notifying her that her Private Information had been impacted during the Fortra Data Breach.

25. Plaintiff Chassidy Holland is, and at all times mentioned herein was, an individual citizen of and residing in the State of Indiana. Plaintiff Holland received a Notice Letter via mail dated March 24, 2023 from CHSPSC notifying her that her Private Information had been impacted during the Fortra Data Breach.

26. Plaintiff Mariana Lopez is, and at all times mentioned herein was, an individual citizen residing in the State of California. Plaintiff Lopez received a Notice

Letter via mail dated February 28, 2023 from Hatch Bank notifying her that her Private Information had been impacted during the Fortra Data Breach.

27. Plaintiff Jennifer Marino is, and at all relevant times mentioned was, an individual citizen of the State of California, except while she briefly resided in Massachusetts from November 2022 to May 2023. Plaintiff Marino received a Notice Letter via mail dated April 27, 2023 from NationsBenefits notifying her that her Private Information had been impacted during the Fortra Data Breach.

28. Plaintiff Melissa Morales is, and at all times mentioned herein was, an individual citizen residing in the State of California. Plaintiff Morales received a Notice Letter via mail dated February 28, 2023 from Hatch Bank notifying her that her Private Information had been impacted during the Fortra Data Breach.

29. Plaintiff Taylor Hartzel Vancosky is, and at all times mentioned herein was, an individual citizen and resident of the State of Pennsylvania. Plaintiff Vancosky received a Notice Letter via mail dated March 24, 2023 from CHSPSC notifying her that her Private Information had been impacted during the Fortra Data Breach.

30. Plaintiff Muhammad Zahid is, and at all times mentioned herein was, an individual citizen and resident of the State of Florida. Plaintiff Zahid received a Notice Letter via mail dated February 28, 2023 from Hatch Bank notifying him that his Private Information had been impacted during the Fortra Data Breach.

FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

31. On its website, Defendant refers to itself as "Your Cybersecurity Ally" and offers services such as vulnerability management, offensive security, email security & Anti-Phishing, Data Protection, Digital Risk Protection, and Secure File Transfer.[7]

32. On information and belief, in the ordinary course of business, Defendant contracts with companies to store and protect client information, such as names and Social Security numbers.

33. On information and belief, Plaintiffs and Class Members provided their Private Information to Fortra's customers who, in turn, hired Defendant to manage access to and store and protect Plaintiffs' and Class Members' Private Information.

34. By accepting and gaining control over Plaintiffs' and Class Members' Private Information, Defendant promised to provide confidentiality and adequate security for this Private Information.

35. By obtaining, controlling, collecting, using, and deriving a benefit from Plaintiffs and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs and Class Members' Private Information from unauthorized disclosure.

36. Plaintiffs and the Class Members have taken reasonable steps to maintain the

[7] https://www.fortra.com/ (last visited: Mar. 6, 2023).

confidentiality of their Private Information.

37. Plaintiffs and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

THE CYBERATTACK AND DATA BREACH

38. Defendant discovered it had been subject to the Data Breach on or around January 29, 2023.

39. On February 3, 2023, Defendant notified its customers that Fortra's systems had been subject to the Data Breach. Specifically, Defendant stated that an actor had gained unauthorized access to Defendant's network through Defendant's applications and, as such, had gained access to Plaintiffs' and the Class's Private Information.

40. The Data Breach is massive in scope. As one journalist stated, "Millions of people across the U.S. had reams of personal and health information stolen in a massive-hack targeting dozens of companies, including healthcare providers[.]"[8] Remarkably, the breach is even more severe than that.

41. By identifying and taking advantage of deficiencies in Fortra's systems, programs, and applications, including a file transfer tool owned, operated, and maintained by Fortra, the GoAnywhere MFT, hackers in a sophisticated ransomware group, either

[8] https://techcrunch.com/2023/05/04/millions-patients-data-stolen-fortra/ (last visited: May 30, 2023).

Clop or TA505, successfully gained access not to just dozens of business's data, but to the data of 130 companies—each of which a Fortra customer.[9]

42. Clop ransomware was first observed in February 2019 in an attack campaign run by Ransomware Group TA505, a known Russian ransomware group that has operated for the past four years and targets aviation, banking, energy, financial, government, healthcare, information technology, manufacturing, retail, technology, and telecommunications. [10]

43. Of note, the Clop ransomware group extorted an average ransom payment of nearly $220,000 per event in the First Quarter of 2021.[11]

44. Specifically, a ransomware group identified a flaw in Fortra's GoAnywhere MFT that enabled them to execute remote codes on Fortra's customers System and create user accounts on the MFT environments—activities that should be possible in a secured environment.[12] With their access to customer environments obtained, the hackers then freely downloaded the Private Information contained within.

---

[9] https://www.bleepingcomputer.com/news/security/fortra-shares-findings-on-goanywhere-mft-zero-day-attacks/ (last visited: May 30, 2023).

[10] https://www.picussecurity.com/resource/clop-ransomware-gang (last visited: May 30, 2023).

[11] *Id.*

[12] https://www.bleepingcomputer.com/news/security/fortra-shares-findings-on-goanywhere-mft-zero-day-attacks/ (last visited: May 30, 2023).

45. In other words, due to vulnerabilities in Fortra's GoAnywhere MFT and deficiencies in its data security posture, hackers were able to gain fully access and control to Fortra's customers MFT environments and all of the data contained therein.

46. Although the full scope of the Data Breach is not yet known by Plaintiffs, the hackers purportedly used these vulnerabilities to gain access to 130 businesses' data, including the Private Information of millions of individuals.[13] This data included highly sensitive information capable of being used in a host of fraudulent schemes, like Plaintiffs' and the Class's Social Security numbers.

47. Fortra's own investigation of the Data Breach confirmed that hackers used vulnerabilities in its GoAnywhere MFT and other aspects of its systems, and that millions of individuals were impacted by the Data Breach.[14]

48. Plaintiffs and Class Members are at significant risk. They provided their Private Information to the Defendant's customers with the reasonable expectation and mutual understanding their information would stay safe. Fortra's customers, who contracted with Fortra and provided them with access to their data, similarly expected that Fortra would keep its promise to use reasonable data security and keep customer data safe.

49. Now, however, Plaintiffs' and the Class's Private Information is in the hands of cybercriminals capable of misusing that data for fraudulent schemes and identity theft.

---

[13] https://www.michigan.gov/ag/news/press-releases/2023/05/16/fortra-data-breach-targets-130-companies-many-in-healthcare-sector (last visited: May 30, 2023).

[14] https://www.fortra.com/blog/summary-investigation-related-cve-2023-0669 (last visited: May 30, 2023).

Although Fortra initially told its customers their data was safe, that was false.[15] Rather, the cybercriminals who orchestrated the attack successfully exfiltrated Plaintiffs' and the Class's data outside of Fortra and its customers' control. That data is now in the hands of criminals who both have the ability to misuse the data for fraud or identity theft, and may also sell it to criminals on the dark web capable of doing the same.

50. This Data Breach was not inevitable. Defendant understood the need to implement reasonable data security given the substantial increase in cyberattacks and/or data breaches preceding the date of the breach.

51. In light of recent high-profile data breaches at other companies similar to Defendant, Defendant knew or should have known that their massive repository of electronic records would be targeted by cybercriminals.

52. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[16]

53. In fact, according to the cybersecurity firm PurpleSec, ransomware "has

---

[15] https://techcrunch.com/2023/03/24/fortra-goanywhere-clop-ransomware/ (last visited: May 30, 2023).

[16] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

become a popular form of attack in recent years growing 350% in 2018," and "up 64% year-over-year" in the first half of 2021.[17]

54. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

55. Defendant, however, utilized inadequate data security and vulnerable remote access and file transfer tools, all of which was exploited to orchestrate the significant theft of data that occurred during the Data Breach.

Defendant Provided Written Notice of the Breach and its Security Failures

56. On or around February 28, 2023, Plaintiffs received a Notice of Security Incident ("Notice of Data Breach"). Fortra did not notify Plaintiffs and the Class directly, but rather, had their customers inform them. The notices provided information about the Data Breach. For instance, the notice from Hatch Bank stated:

> **What Happened?** On January 29, 2023, Fortra experienced a cyber incident when they learned of a vulnerability located in their software. On February 3, 2023, Hatch Bank was notified by Fortra of the incident and learned its files contained on Fortra's GoAnywhere site were subject to unauthorized access. Fortra's investigation determined that, between January 30 and January 31, 2023, someone without authorization had access to certain files stored within Fortra's GoAnywhere site. Fortra launched a diligent and comprehensive review of relevant files to determine the information that may have been impacted.

---

[17] *2021 Cyber Security Statistics, The Ultimate List of Stats, Data, & Trends for 2023*, https://purplesec.us/resources/cyber-security-statistics/#Ransomware (last visited Mar. 15, 2023).

> **What Information was Involved?** On February 7, 2023, Fortra determined the information may have been impacted by this incident includes [Plaintiff's] name and Social Security number. Again, at this time Fortra has no indication that your information was subject to an actual or attempted misuse as a result of this incident.

57. Through its Notice of Data Breach, Defendant admits that the Data Breach was caused, at least in part, due to "vulnerability[ies] located in [its] software."

58. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

The Data Breach Was Foreseeable

59. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

60. It is well known that PII, including social security numbers in particular, is an invaluable commodity and a frequent target of hackers.

61. In 2019, a record 1,473 data breaches occurred, resulting in approximately

164,683,455 sensitive records being exposed, a 17% increase from 2018.

62. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

63. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and the putative Class Members from being compromised.

Value of PII

64. Consumers place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

65. Consumers are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[18] There are long-term consequences to data

[18] https://www.kiplinger.com/article/credit/t048-c011-s001-how-to-protect-your-kids-from-the-anthem-data-brea.html (last visited: May 29, 2023).

breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."

66. The PII of consumers remains of high value to criminals, as evidenced by the prices offered through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[19]

67. According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[20] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[21]

---

[19] *Your personal data is for sale on the Dark Web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[20] Zachary Ignoffo, *Dark Web Price Index 2021*, PRIVACY Affairs (Mar. 8, 2021), https://www.privacyaffairs.com/dark-web-price-index-2021/.

[21] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

68. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[22]

69. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

70. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security

[22] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

number."[23]

71. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[24]

72. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[25]

73. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.

---

[23] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[24] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[25] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last visited November 2, 2021)

> Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[26]

74. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[27] However, this is not the case. As cybersecurity experts point out:

> It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.[28]

75. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[29]

76. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in

---

[26] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?* (October 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited: November 2, 2021).

[27] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited: November 2, 2021).

[28] *Id.*

[29] *How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited: November 2, 2021).

combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[30]

77. Given the nature of the Data Breach, it is foreseeable that the compromised Private Information can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Class Members' Private Information can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

78. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

79. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

80. The fraudulent activity resulting from the Data Breach may not come to light for years.

[30] See OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1 (May 22, 2007), available at https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2007/m07-16.pdf.

81. There is also a robust legitimate market for the type of sensitive information at issue here. Marketing firms utilize personal information to target potential customers, and an entire economy exists related to the value of personal data.

82. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

83. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[31]

84. As such, future monitoring of financial and personal records is reasonable and necessary well beyond the one year of protection offered by Defendant.

Defendant Failed to Comply with FTC Guidelines

[31] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited: Aug. 23, 2021).

85. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

86. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[32] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[33]

87. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested

---

[32] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, (2016). Available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

[33] *Id.*

methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

88. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

89. Defendant failed to properly implement basic data security practices.

90. Defendant's failure to employ reasonable and appropriate measures to protect against and detect unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

91. Defendant was at all times fully aware of its obligation to protect the Private Information of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

92. As shown above, several best practices have been identified that should, at a minimum, be implemented by businesses like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backing up data; limiting which employees can access sensitive data;

and testing its systems and applications for exploitable vulnerabilities.

93. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protecting against any possible communication system; and training staff on critical points.

94. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

95. These frameworks are existing and applicable industry standards in any industry. Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

Defendant's Breach

96. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it implemented unreasonable and deficient data security to safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Maintaining an inadequate data security system to reduce the risk of data breaches and cyberattacks;

b. Inadequately protecting customers' Private Information;

c. Improperly monitoring its own data security systems for existing intrusions;

d. Using inadequate measures to ensure its vendors with access to its computer systems and data employed reasonable security procedures;

e. Inadequately training its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Implementing deficient policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

g. Implementing insufficient procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

h. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

i. Implementing data security measures that were below and incompliant with industry standards for cybersecurity.

97. Defendant negligently and unlawfully failed to safeguard Plaintiffs and Class Members' Private Information by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted Private Information.

98. Accordingly, as outlined below, Plaintiffs and Class Members now face a present and substantially increased risk of fraud and identity theft. In addition, Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendant.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at a Present and Substantially Increased Risk of Fraud and Identity Theft

99. Cyberattacks and data breaches at companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

100. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[34]

101. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal Private Information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identify thieves who desire to extort and harass victims, take over

[34] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

102. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[35]

103. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

---

[35] *See* Federal Trade Commission, *IdentityTheft.gov*, https://www.identitytheft.gov/#/Steps (last visited: Aug. 25, 2021).

104. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

105. Moreover, theft of Private Information is also gravely serious. Private Information is an extremely valuable property right.[36]

106. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

107. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

108. There is a strong probability that entire batches of information stolen from

---

[36] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

Defendant have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at a present and substantially increased risk of fraud and identity theft for many years into the future.

109. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

110. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[37] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

111. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[38] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[39] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law

---

[37] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[38] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1, available at https://www.ssa.gov/pubs/EN-05-10064.pdf.

[39] *Id.* at 4.

enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

Defendant Failed to Properly Protect Plaintiffs' and Class Members' Private Information

112. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

113. Defendant never encrypted or redacted Plaintiff's and Class Members Private Information. Had this information been properly encrypted, the cybercriminals would have not been able to decipher any of the information.

114. Defendant, furthermore, could have prevented the Data Breach by performing standard, well-established vulnerability testing to evaluate deficiencies in its own applications that were later used, in part, to orchestrate the Data Breach.

115. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies and educational organizations like Defendant to protect and secure sensitive data they possess.

116. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

117. The Federal Trade Commission ("FTC") defines identity theft as "a fraud

committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[40]

118. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once PII or PHI is stolen, fraudulent use of that information and damage to victims may continue for years.

119. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

[40] *See generally* https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last visited: October 21, 2022).

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[41]

[41] *Id.* at 3-4.

120. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce

malicious network traffic….[42]

121. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

[42] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Aug. 23, 2021).

Apply principle of least-privilege

- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection;
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[43]

122. Given that Defendant was storing the Private Information of Plaintiffs and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

123. Moreover, given that Defendant was storing the Private Information of Plaintiffs and Class Members on a separate server, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

124. The occurrence of the Data Breach indicates that Defendant failed to

[43] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Aug. 23, 2021).

adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiffs and Class Members.

125. As a result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

126. Because Defendant failed to properly protect and safeguard Plaintiff's and Class Members' Private Information, an unauthorized third party was able to access Defendant's network, and access Defendant's database and system configuration files and exfiltrate that data.

PLAINTIFF-SPECIFIC ALLEGATIONS

Plaintiff Valerie Anderson

127. Plaintiff Anderson is a consumer affiliated with Hatch Bank, which, on information and belief, obtained Plaintiff Anderson's Private Information in order to provide her lending services. Upon information and belief, Hatch Bank contracted with Defendant to store and/or transfer Plaintiffs' and Class Members' Private Information.

128. On or about early March 2023, Plaintiff Anderson received a Notice of Data Breach from Hatch Bank, informing her that her Private Information, including her name and Social Security number, was compromised by Fortra's Data Breach.

129. As a result of the Data Breach, Defendant directed Plaintiff Anderson to take

certain steps to protect her Private Information and otherwise mitigate her damages.

130. Since the Data Breach, Plaintiff Anderson has experienced fraudulent charges on her PayPal account and a significant increase in spam calls and emails. Fortra's Data Breach remains the most likely cause of the fraudulent charge given its close proximity to the fraud and its logical connection, that is, because the information stolen in the Data Breach could be used to commit this type of fraud.

131. As a result of the Data Breach, Plaintiff Anderson has spent significant time dealing with the consequences of the Data Breach including: self-monitoring her bank and credit accounts; verifying the legitimacy of potentially fraudulent charges; communicating with her bank, exploring credit monitoring and identity theft insurance options; and signing up for the credit monitoring offered by Defendant.

132. Plaintiff Anderson is very careful about sharing her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

133. Plaintiff Anderson stores any and all documents containing Private Information in a secure location, and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

134. Plaintiff Anderson has suffered, and continues to suffer, a loss of privacy as a result of the Data Breach.

135. Plaintiff Anderson has been deprived of the value of her Private Information, the value of which is largely derived from the fact that it is private.

136. Plaintiff Anderson is alarmed by the amount of her Personal Information that was stolen or accessed—in particular the combination of her full name and Social Security number—and suffers from stress and anxiety due to the loss of privacy and the substantial risk of additional harm that she faces as a result of the Data Breach.

137. Plaintiff Anderson has a continuing interest in ensuring that her Private Information, which likely remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Danielle Adams

138. Upon information and belief, Brightline Medical Associates is an affiliate of Comcast NBCUniversal ("Comcast") and has contracted with Comcast to provide certain medical services to Comcast employees and their families. Plaintiff Adams' husband is an employee of Comcast. Upon information and belief, Brightline obtained Plaintiff Adams' Private Information (as well as the Private Information of her husband and minor child) in the ordinary course of its relationship with Comcast. Upon information and belief, Brightline contracted with Defendant to store and/or transfer Plaintiffs' and Class Members' Private Information.

139. On or about April 21, 2023, Plaintiff Adams received a Notice of Data Breach from Brightline informing her that her Private Information, including her first and last name, date of birth, sex, employer, subscriber ID, member ID, Group ID, address,

email address, coverage start and end dates, and Social Security number, were compromised in the Data Breach.

140. As a result of the Data Breach, Defendant directed Plaintiff Adams to take certain steps to protect her Private Information and otherwise mitigate her damages.

141. Following the Data Breach, Plaintiff Adams received notification from a third-party service that her information was located on the dark web.

142. As a result of the Data Breach, Plaintiff has spent approximately 15 hours attempting to mitigate consequences from the substantial risk of additional harm that her and her family face as a result of the Data Breach. For example, Plaintiff Adams spent significant time signing up for the limited credit monitoring services offered by Brightline, obtaining a credit freeze for her and her husband, reviewing the financial accounts belonging to her and her family, speaking with a credit bureau related to a suspicious entry on her minor child's credit report, and traveling to her bank to discuss account security and change her passwords.

143. Plaintiff has also incurred costs attempting to mitigate the substantial risk of additional harm to her and her family from the Data Breach. For example, after receiving the notice from Brightline, Plaintiff missed three hours of work attempting perform tasks described above. This caused her to lose approximately $51 in wages. Plaintiff Adams was also required to purchase an application on her cell phone that allowed her to fax relevant documents to a credit bureau. The application cost approximately $10. To use this application, Plaintiff Adams first had to print out the relevant document using her own

paper and ink. Lastly, Plaintiff Adams was forced to consume the gasoline in her vehicle when traveling to the bank to discuss issues related to the Data Breach.

144. Plaintiff Adams is very careful about sharing her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

145. Plaintiff Adams stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her banking and other sensitive online accounts.

146. Plaintiff Adams has suffered, and continues to suffer, a loss of privacy as a result of the Data Breach.

147. Plaintiff Adams has been deprived of the value of her Private Information, the value of which is largely derived from the fact that it is private.

148. Plaintiff Adams is alarmed by the amount of her and her family's Private Information that was stolen or accessed and suffers from stress and anxiety due to the loss of privacy and the substantial risk of additional harm that her and her family face as a result of the Data Breach.

149. Plaintiff Adams has a continuing interest in ensuring that her Private Information, which likely remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Theresa Brewerton

150. Plaintiff Brewerton is a patient affiliated with NationsBenefits Holdings, LLC, which obtained Plaintiff Brewerton's Private Information in order to provide her health insurer with administrative services. Upon information and belief, NationsBenefits Holdings, LLC, contracted with Defendant to store and/or transfer Plaintiffs' and Class Members' Private Information

151. On or about April 27, 2023, Plaintiff Brewerton received a Notice of Data Breach from NationsBenefits, LLC, informing her that her Private Information, including her full name (including middle initial), gender, Health Plan Subscriber Identification Number, address, phone number, date of birth, and Medicare Number, was compromised by the Data Breach.

152. As a result of the Data Breach, Defendant directed Plaintiff Brewerton to take certain steps to protect her Private Information and otherwise mitigate her damages. Plaintiff Brewerton followed this advice. For example, she spent several hours researching information related to the Data Breach.

153. Following the Data Breach, Plaintiff Brewerton was notified that her information was located on the dark web. Furthermore, Plaintiff Brewerton suffered an attempted fraudulent charge on her debit card. As a result, her bank cancelled her card, which she did not find out about until her card was declined while attempting to pump gasoline for her vehicle, leaving her unable to do so at that time. Thereafter, Plaintiff Brewerton had to drive to her bank to have her debit card replaced, causing her to consume

gasoline in her vehicle. As a result of her card cancellation, Plaintiff Brewerton was also forced to spend significant time resetting her automatic billing instructions.

154. Fortra's Data Breach remains the most likely cause of the attempted fraudulent charge given its close proximity to the fraud and its logical connection, that is, because the information stolen in the data breach could be used to commit this type of fraud.

155. Plaintiff Brewerton is very careful about sharing her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

156. Plaintiff Brewerton stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for his/her various online accounts.

157. Plaintiff Brewerton has suffered, and continues to suffer, a loss of privacy as a result of the Data Breach.

158. Plaintiff Brewerton has been deprived of the value of her Private Information, the value of which is largely derived from the fact that it is private.

159. Plaintiff Brewerton is alarmed by the amount of her Personal Information that was stolen or accessed and suffers from stress and anxiety due to the loss of privacy and the substantial risk of additional harm that she faces as a result of the Data Breach.

160. Plaintiff Brewerton has a continuing interest in ensuring that her Private Information, which likely remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Joseph Cardenas

161. Plaintiff Cardenas' Private Information was obtained by Fortra through Brightline.

162. On or about April 7, 2023, Plaintiff Cardenas received a Notice of Data Breach from Brightline, informing him that his Private Information, including his full name, address, member ID, date of birth, phone number, employer's name, his employer's group ID number, and his coverage and start dates, was compromised by the Data Breach.

163. As a result of the Data Breach, Defendant directed Plaintiff Cardenas to take certain steps to protect his Private Information and otherwise mitigate his damages. Plaintiff Cardenas followed this advice, spending significant time reviewing his financial accounts, reviewing his credit report, and changing his passwords.

164. Following the Data Breach, Plaintiff Cardenas has experienced a significant increase in phishing text messages.

165. Plaintiff Cardenas is very careful about sharing his Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

166. Plaintiff Cardenas stores any and all documents containing Private

Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

167. Plaintiff Cardenas has suffered, and continues to suffer, a loss of privacy as a result of the Data Breach.

168. Plaintiff Cardenas has been deprived of the value of his Private Information, the value of which is largely derived from the fact that it is private.

169. Plaintiff Cardenas is alarmed by the amount of his Personal Information that was stolen or accessed, and suffers from stress and anxiety due to the loss of privacy and the substantial risk of additional harm that he faces as a result of the Data Breach.

170. Plaintiff Cardenas has a continuing interest in ensuring that his Private Information, which likely remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Linda Caudill

171. Plaintiff Linda Caudill is a consumer affiliated with Hatch Bank, which, on information and belief, obtained Plaintiff Caudill's Private Information in order to provide her lending services. Upon information and belief, Hatch Bank contracted with Defendant to store and/or manage Plaintiffs' and Class Members' Private Information.

172. On or about early March 2023, Plaintiff Caudill received a Notice of Data Breach from Hatch Bank, informing her that her Private Information, including her name

and Social Security number, was compromised by the Data Breach.

173. As a result of the Data Breach, Defendant directed Plaintiff Caudill to take certain steps to protect her Private Information and otherwise mitigate her damages.

174. Since the Data Breach, Plaintiff Caudill has experienced a significant increase in spam calls.

175. As a result of the Data Breach, Plaintiff Caudill has spent significant time dealing with the consequences of the Data Breach including signing up for credit monitoring offered by Defendant, regularly monitoring her account and credit reports, checking with the IRS for potentially fraudulent returns. Plaintiff Caudill also paid for gas to drive herself to her bank to meet with a representative to discuss her accounts and the ways to mitigate the impact of the data breach.

176. Plaintiff Caudill is very careful about sharing her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

177. Plaintiff Caudill stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

178. Plaintiff Caudill has suffered, and continues to suffer, a loss of privacy as a result of the Data Breach.

179. Plaintiff Caudill has been deprived of the value of her Private Information, the value of which is largely derived from the fact that it is private.

180. Plaintiff Caudill is alarmed by the amount of her Personal Information that was stolen or accessed—in particular the combination of her full name and Social Security number—and suffers from stress and anxiety due to the loss of privacy and the substantial risk of additional harm that she faces as a result of the Data Breach.

181. Plaintiff Caudill has a continuing interest in ensuring that her Private Information, which likely remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Chassidy Holland

182. Plaintiff Holland is a patient affiliated with CHSPSC, which obtained Plaintiff Holland's Private Information in order to provide her with medical services. Upon information and belief, CHSPSC contracted with Defendant to store and/or transfer Plaintiffs' and Class Members' Private Information

183. In or about late March 2023, Plaintiff Holland received a Notice of Data Breach from CHSPSC, informing her that her Private Information, including her full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as her date of birth and Social Security number was compromised by the Data Breach.

184. As a result of the Data Breach, Defendant directed Plaintiff Holland to take certain steps to protect her Private Information and otherwise mitigate her damages.

185. Since the Data Breach, Plaintiff Last Holland has had multiple instances of fraud including: unauthorized charges on her bank and credit card, unauthorized orders on her amazon account, fraudulent applications for loans and credit cards, a fraudulent tax return filed for her daughter, and her information has been found on the dark web. Fortra's Data Breach remains the most likely cause of the fraud given its close proximity to the fraud and its logical connection, that is, because the information stolen in the data breach could be used to commit this type of fraud.

186. As a result of the Data Breach, Plaintiff Holland has spent significant time dealing with the consequences of the Data Breach including: self-monitoring her bank and credit accounts; verifying the legitimacy of potentially fraudulent charges; and will be freezing her credit. Plaintiff Holland experienced a substantial drop in her credit score, signed up and paid for Experian credit monitoring. Plaintiff Holland also had to pay for gas to visit the bank and had trouble paying for her father's funeral expenses as a result of the identity theft.

187. Plaintiff Holland is very careful about sharing her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

188. Plaintiff Holland stores any and all documents containing Private Information in a secure location, and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently

chooses unique usernames and passwords for her various online accounts.

189. Plaintiff Holland has suffered, and continues to suffer, a loss of privacy as a result of the Data Breach.

190. Plaintiff Holland has been deprived of the value of her Private Information, the value of which is largely derived from the fact that it is private.

191. Plaintiff Holland is alarmed by the amount of her Personal Information that was stolen or accessed, and suffers from stress and anxiety due to the loss of privacy and the substantial risk of additional harm that she faces as a result of the Data Breach.

192. Plaintiff Holland has a continuing interest in ensuring that her Private Information, which likely remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Mariana Sanchez Lopez

193. Plaintiff Lopez is a consumer affiliated with Hatch Bank which, on information and belief, obtained Plaintiff Lopez's Private Information, including her name, date of birth, phone number, email address, and Social Security number, when she applied for a loan with one of its affiliates. Upon information and belief, Hatch Bank contracted with Defendant to store and/or transfer Plaintiff Lopez's and Class Members' Private Information.

194. On or about February 28, 2023, Plaintiff Lopez received a Notice of Data Breach from Hatch Bank, informing her that her Private Information, including her name and Social Security number, was compromised by the Data Breach.

195. As a result of the Data Breach, Defendant directed Plaintiff Lopez to take certain steps to protect her Private Information and otherwise mitigate her damages. For example, Plaintiff Lopez has spent several hours reviewing her financial accounts and credit reports. Plaintiff Lopez also attempted to register for the free credit monitoring service offered by Hatch Bank. However, the link provided in her notice letter was invalid, leaving her unable to register her account. Therefore, Plaintiff Lopez was forced to rely on a third-party service to inspect her credit and ensure that she had not already suffered identity theft.

196. Plaintiff Lopez is very careful about sharing her Private Information and generally does not knowingly transmit unencrypted Private Information over the internet or any other unsecured source.

197. Plaintiff Lopez stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

198. Plaintiff Lopez has suffered, and continues to suffer, a loss of privacy as a result of the Data Breach.

199. Plaintiff Lopez has been deprived of the value of her Private Information, the value of which is largely derived from the fact that it is private.

200. Plaintiff Lopez is alarmed by the amount of her Private Information that was

stolen or accessed and suffers from stress and anxiety due to the loss of privacy and the substantial risk of additional harm that she faces as a result of the Data Breach.

201. Plaintiff Lopez has a continuing interest in ensuring that her Private Information, which likely remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Jennifer Marino

202. Plaintiff Jennifer Marino is a patient affiliated with NationsBenefits Holdings, LLC, who obtained Plaintiff Marino's Private Information in order to provide his/her health insurer with administrative services. Upon information and belief, NationsBenefits Holdings, LLC, contracted with Defendant to store and/or transfer Plaintiffs' and Class Members' Private Information

203. On or about late April to early May 2023, Plaintiff Marino received a Notice of Data Breach from NationsBenefits, LLC, informing her that her Private Information, including her first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, date of birth and Medicare number had been impacted by the Data Breach.

204. As a result of the Data Breach, Defendant directed Plaintiff Marino to take certain steps to protect her Private Information and otherwise mitigate her damages.

205. Since the Data Breach, Plaintiff Marino has experienced a significant increase in spam calls and emails.

206. As a result of the Data Breach, Plaintiff Marino has spent significant time

dealing with the consequences of the Data Breach including: self-monitoring her bank and credit accounts; and researching credit monitoring and identity theft insurance options.

207. Plaintiff Marino is very careful about sharing her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

208. Plaintiff Marino stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

209. Plaintiff Marino has suffered, and continues to suffer, a loss of privacy as a result of the Data Breach.

210. Plaintiff Marino has been deprived of the value of her Private Information, the value of which is largely derived from the fact that it is private.

211. Plaintiff Marino is alarmed by the amount of her Personal Information that was stolen or accessed and suffers from stress and anxiety due to the loss of privacy and the substantial risk of additional harm that she faces as a result of the Data Breach.

212. Plaintiff Marino has a continuing interest in ensuring that her Private Information, which likely remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Melissa Morales

213. Plaintiff Melissa Morales is a consumer affiliated with Hatch Bank which, on information and belief, obtained Plaintiff Morales' Private Information, including her name, date of birth, phone number, email address, and Social Security number, when she applied for a loan with one of its affiliates. Upon information and belief, Hatch Bank contracted with Defendant to store and/or transfer Plaintiff Morales' and Class Members' Private Information.

214. On or about February 28, 2023, Plaintiff Morales received a Notice of Data Breach from Hatch Bank, informing her that her Private Information, including her name and Social Security number, was compromised by the Data Breach.

215. As a result of the Data Breach, Defendant directed Plaintiff Morales to take certain steps to protect her Private Information and otherwise mitigate her damages. For example, she has spent multiple hours reviewing her financial accounts and credit reports.

216. Following the Data Breach, Plaintiff Morales was notified by a third-party monitoring service that her Social Security number was located on the dark web. She has also experienced a significant increase in the amount of spam and phishing communications that she has received.

217. Following the Data Breach, someone used Plaintiff Morales' name and date of birth to obtain medicine that was prescribed to her from her pharmacy. As a result of this fraud, Plaintiff Morales had to spend significant time on the phone with her pharmacy. Plaintiff Morales was also required to make multiple in person visits to her pharmacy,

causing her to consume gasoline that she paid for. In total, Plaintiff Morales was required to spend more than three hours dealing with this fraud.

218. Fortra's Data Breach remains the most likely cause of the medical fraud given its close proximity to the fraud and its logical connection, that is, because the information stolen in the data breach could be used to commit this type of fraud.

219. Plaintiff Morales is very careful about sharing her Private Information and generally does not knowingly transmit unencrypted Private Information over the internet or any other unsecured source.

220. Plaintiff Morales stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

221. Plaintiff Morales has suffered, and continues to suffer, a loss of privacy as a result of the Data Breach.

222. Plaintiff Morales has been deprived of the value of her Private Information, the value of which is largely derived from the fact that it is private.

223. Plaintiff Morales is alarmed by the amount of her Private Information that was stolen or accessed and suffers from stress and anxiety due to the loss of privacy and the substantial risk of additional harm that she faces as a result of the Data Breach.

224. Plaintiff Morales has a continuing interest in ensuring that her Private

Information, which likely remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Tara Hartzel Vancosky

225. Plaintiff Tara Hartzel Vancosky is a patient affiliated with CHSPSC, which obtained Plaintiff Vancosky's Private Information in order to provide her with medical services. Upon information and belief, CHSPSC contracted with Defendant to store and/or transfer Plaintiffs' and Class Members' Private Information

226. On or about late March 2023, Plaintiff Vancosky received a Notice of Data Breach from CHSPSC, informing her that her Private Information, including her full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as her date of birth and Social Security number, was compromised by the Data Breach.

227. As a result of the Data Breach, Defendant directed Plaintiff Vancosky to take certain steps to protect her Private Information and otherwise mitigate her damages.

228. Since the Data Breach, Plaintiff Vancosky has experienced an increase in spam calls.

229. As a result of the Data Breach, Plaintiff Vancosky has spent a significant amount of time monitoring her accounts for fraudulent transactions, taking spam calls, and transferring funds.

230. Plaintiff Vancosky is very careful about sharing her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any

other unsecured source.

231. Plaintiff Vancosky stores any and all documents containing Private Information in a secure location, and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

232. Plaintiff Vancosky has suffered, and continues to suffer, a loss of privacy as a result of the Data Breach.

233. Plaintiff Vancosky has been deprived of the value of her Private Information, the value of which is largely derived from the fact that it is private.

234. Plaintiff Vancosky is alarmed by the amount of her Personal Information that was stolen or accessed, and suffers from stress and anxiety due to the loss of privacy and the substantial risk of additional harm that she faces as a result of the Data Breach.

235. Plaintiff Vancosky has a continuing interest in ensuring that her Private Information, which likely remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Muhammad Zahid

236. Plaintiff Muhammad Zahid is a consumer affiliated with Hatch Bank which, on information and belief, obtained Plaintiff Zahid's Private Information in order to provide him lending services. Upon information and belief, Hatch Bank contracted with Defendant to store and/or transfer Plaintiffs' and Class Members' Private Information.

237. On or about early March 2023, Plaintiff Zahid received a Notice of Data Breach from Hatch Bank informing him that his Private Information, including his name and Social Security number, was compromised by the Data Breach.

238. As a result of the Data Breach, Defendant directed Plaintiff Zahid to take certain steps to protect his Private Information and otherwise mitigate his damages.

239. Since the Data Breach, Plaintiff Zahid has an increase in spam calls, texts, and emails.

240. As a result of the Data Breach, Plaintiff Zahid has spent a significant amount of time monitoring his financial accounts and placing credit freezes.

241. Plaintiff Zahid is very careful about sharing his Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

242. Plaintiff Zahid stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

243. Plaintiff Zahid has suffered, and continues to suffer, a loss of privacy as a result of the Data Breach.

244. Plaintiff Zahid has been deprived of the value of his Private Information, the value of which is largely derived from the fact that it is private.

245. Plaintiff Zahid is alarmed by the amount of his Personal Information that was stolen or accessed, and suffers from stress and anxiety due to the loss of privacy and the substantial risk of additional harm that he faces as a result of the Data Breach.

246. Plaintiff Zahid has a continuing interest in ensuring that his Private Information, which likely remains in Defendant's possession, is protected and safeguarded from future breaches.

Injuries and Damages Common to Plaintiffs

247. As a result of Defendant's mismanagement of their Private Information, Plaintiffs have suffered actual injury and damages.

248. Plaintiffs suffered actual injury in the form of damages and diminution in the value of their Private Information—a form of intangible property that they either directly or indirectly entrusted to Defendant, which was compromised in and as a result of the Data Breach.

249. As a result of the Data Breach and the information that they received in the Notice Letter, Plaintiffs have spent significant time dealing with the consequences of the Data Breach, such as self-monitoring their bank and credit accounts, spending time verifying the legitimacy of communications with their banks, exploring credit monitoring and identity theft insurance options, and signing up for the credit monitoring supplied by Defendant. This time has been lost forever and cannot be recaptured.

250. Plaintiffs suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and have suffered anxiety and increased concerns for the theft of

their privacy since they received a Notice Letter. They are especially concerned about the theft of their full names paired with their Social Security numbers.

251. Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their stolen Private Information, especially their Social Security numbers, being placed in the hands of unauthorized third parties and possibly criminals.

252. Plaintiffs have a continuing interest in ensuring that their Private Information, which likely remains in Defendant's possession, is protected and safeguarded from future breaches.

253. To date, Defendant has done nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

254. Defendant has merely offered Plaintiffs and Class Members complimentary fraud and identity monitoring services for up to twelve months, but this does nothing to compensate them for damages already incurred, those that could potentially arise from future misuse of their leaked Private Information, nor the time they have spent and will continue to spend dealing with the Data Breach.

255. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

256. Plaintiffs' Private Information was compromised in the Data Breach and is now in the hands of, at the very least, the cybercriminals who accessed Defendant's computer system.

257. Plaintiffs' Private Information was compromised as a direct and proximate result of the Data Breach.

258. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of fraud and identity theft, among others.

259. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time addressing the effects of the Data Breach in attempt to minimize their losses.

260. Plaintiffs and Class Members face the present and substantially increased risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar forms of identity theft.

261. Plaintiffs and Class Members face the present and substantially increased risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information, as potential fraudsters could use that information to more effectively target Plaintiffs and Class Members in future schemes.

262. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

263. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts

have recognized the propriety of loss of value damages in related cases.

264. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service or product that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer network and Plaintiffs and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for and agreed to.

265. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their medical accounts and sensitive information for misuse.

266. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

267. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

268. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

CLASS ACTION ALLEGATIONS

269. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

270. Plaintiffs propose the following Nationwide Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised as a result of the Data Breach, including those who were sent a Notice of Data Breach (the "Nationwide Class").

271. Alternatively, Plaintiffs Marino, Morales, and Lopez seek to represent the following sub-class of California residents as follows:

> All California residents whose Private Information was compromised as a result of the Data Breach, including those who were sent a Notice of Data Breach (the "California Sub-Class").

272. Unless otherwise specified, the proposed Nationwide Class and California Sub-Classes are referred to collectively as the "Class." Members of the Nationwide Class and Sub-Class are referred to collectively as "Class Members."

273. Excluded from the Class and Sub-Classes are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class and Sub-classes are members of the judiciary to whom this case is assigned, their families and Members of their staff.

274. Plaintiffs reserve the right to amend or modify the Class definitions as this case progresses.

275. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of approximately 139,493 individuals whose Private Information was compromised in the Data Breach.

276. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached a fiduciary duty to Plaintiffs and Class Members;

l. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

m. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, treble damages, and/or injunctive relief.

277. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

278. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

279. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all of Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action advances the interests of judicial economy, among others.

280. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law

and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. In contrast, litigating this matter as a class action presents far fewer management difficulties, conserves judicial and party resources, and protects the rights of each Class Member.

281. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and All Nationwide Class Members)

282. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

283. Defendant required Plaintiffs and Class Members to submit non-public personal information as a condition of employment (or prospective employment) and willingly solicited, obtained from its customers, and took responsibility for the Private Information of Plaintiffs' and Class members.

284. Defendant had a duty to exercise reasonable care in collecting and storing this data, including using reasonable means to secure and safeguard its computer systems—

and the Class Members' Private Information held within them—from unauthorized disclosure, as well as to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

285. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

286. Defendant owed this duty to Plaintiffs and the Class because Plaintiffs and the Class are a well-defined, foreseeable, and probable group of individuals whom Defendant knew or should have known could be injured by its inadequate data security. Defendant actively solicited clients who owned, stored, and maintained Private Information and, as part of its services, Defendant took control and managed that Private Information on behalf of its clients. Thus, for Defendant to provide its services, Defendant was required to manage, use, handle, gather, and store the Private Information of Plaintiffs and Class Members. A repository of highly Private Information was a significant target for hackers. Defendant, thus, knew and understood long before the Data Breach that, as the keeper and manager of a significant volume of Private Information, it would need to implement adequate data security measures to protect against a Data Breach. The

foreseeable harm to Plaintiff and the Class of Defendant's inadequate data security measures created a duty to act reasonably in securing the Private Information it oversaw.

287. Defendant's duty of care to use reasonable security measures separately arose because Defendant assumed a duty when it voluntarily took responsibility for Plaintiffs' and Class Members' Private Information. Defendant represented to its clients that it could collect, manage, store, and secure their customers' data and keep it safe. As such, when those clients provided Defendant with responsibility to manage and protect customers' Private Information, it obligated Defendant to use reasonable measures to protect, secure, and prevent the theft of that information against the foreseeable threat of a data breach.

288. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data. 15 U.S.C. § 45.

289. Defendant breached its duties, and was thus negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain reasonably adequate security measures to safeguard Class Members' Private Information;

b. Failing to reasonably monitor the security of their networks and systems;

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Cyber-Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages

290. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the well-known high frequency of cyberattacks and data breaches in the past few years.

291. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in injury to Class Members.

292. Plaintiffs and Class Members are entitled to damages as a result of the Data Breach.

293. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and All Nationwide Class Members)

294. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

295. Pursuant to Section 5 of the Federal Trade Commission Act, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information. 15 U.S.C. § 45.

296. Plaintiffs and Class Members are within the class of persons that the FTCA was intended to protect.

297. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The Federal Trade Commission ("FTC") has pursued enforcement actions against businesses that, due to their failure to employ reasonable data security measures and abstain from unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class here.

298. Defendant breached its duties to Plaintiffs and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

299. Defendant's violations of the FTCA constitute negligence *per se.*

300. But for Defendant's negligent breach of the duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

301. The injury and harm suffered by Plaintiffs and Class Members was a reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was acting in violation of the law and in breach of its duties, and that such breaches would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

302. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Declaratory Judgment
(On Behalf of Plaintiffs and All Nationwide Class Members)

303. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

304. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

305. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard its the Private Information at issue and whether Defendant currently maintains data security

measures adequate to protect Plaintiffs and Class Members from further data breaches that threaten the Private Information in Defendant's possession.

306. Plaintiffs allege that Defendant's data security measures remain inadequate. Plaintiffs and Class Members will continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

307. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, that Defendant:

a. Continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes.

b. Continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

308. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ reasonable security protocols consistent with law and industry standards to protect consumers' Private Information.

309. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach. The risk of another data breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and Class Members will not have an adequate remedy at law because

many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

310. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Defendant, Plaintiffs and Class Members will likely be subjected to increased fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

311. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised.

COUNT IV
CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, *et seq.*
(On Behalf of Plaintiffs Morales, Lopez, Marino, and the California Sub-Class Members)

312. Plaintiffs Morales, Lopez, and Marino, individually and on behalf of the California Sub-class, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

313. "To ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

314. Defendant is a business that owns, maintains, and licenses Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiffs Morales, Lopez, Marino, and the California Sub-Class. Businesses that own or license computerized data that includes PII, including Social Security numbers, medical information, and health information, are required to notify California residents when their PII has been acquired (or reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

315. Defendant is a business that owns or licenses computerized data that includes PII as defined by Cal. Civ. Code § 1798.82.

316. By virtue of its business relationships, Defendant licensed computerized data that contained PII as defined by Cal. Civ. Code § 1798.82.

317. In the alternative, Defendant maintains computerized data that includes PII as defined by Cal. Civ. Code § 1798.82.

318. As a business that "owned or licensed computerized data with PII" or, in the alternative, "maintain[ed] computer data with PII," Defendant had a duty to notify California Sub-Class Members of the Data Breach.

319. Plaintiffs Morales, Lopez, Marino, and California Sub-Class Members' Private Information includes PII as covered by Cal. Civ. Code § 1798.82.

320. Because Defendant reasonably believed that Plaintiffs' and California Sub-Class Members' PII was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

321. Defendant failed to send notice of the Data Breach under Cal. Civ. Code § 1798.92 to any California Sub-Class Member.

322. Moreover, even if Defendant's notice obligation is excused by virtue of its customers issuing notice, Defendant still violated Cal. Civ. Code § 1798.92 because it failed to fully disclose material information about the Data Breach, including, but not limited to, the fact that the Data Breach arose from a ransomware attack.

323. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Cal. Civ. Code § 1798.82.

324. As a direct and proximate result of Defendant's violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs Morales, Lopez, Marino, and California Sub-class Members suffered damages as described above.

325. Plaintiffs Morales, Lopez, Marino, and California Sub-Class Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT V
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW
Cal. Bus. Code § 17200, *et seq.*
(On Behalf of Plaintiffs Morales, Lopez, Marino, and the California Sub-class Members)

326. Plaintiffs Morales, Lopez, and Marino, individually and on behalf of the California Sub-Class, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

327. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq.* which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL")

328. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, et seq. (the "CCPA"), and other state data security laws.

329. Defendant stored the Private Information of Plaintiffs and the California Sub-Class and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would

have kept Plaintiffs' and the California Sub-class's Private Information secure and prevented the loss or misuse of that PII.

330. Defendant also violated California Civil Code § 1798.150 by failing to employ reasonable security measures, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and the California Sub-class's Private Information.

331. Had Defendant complied with these requirements, Plaintiffs and the California Sub-Class would not have suffered the damages related to the data breach.

332. Defendant's conduct was unlawful, in that it violated the Consumer Records Act, among other statutory and common laws.

333. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

334. Defendant's conduct was an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting and taking responsibility for the safeguarding of PII.

335. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal.

Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.").

336. Instead, Defendant made the Private Information of Plaintiffs and the Sub-Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiffs and the Sub-Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

337. As a result of those unlawful and unfair business practices, Plaintiffs and the Sub-Class suffered an injury-in-fact and have lost money or property.

338. The injuries to Plaintiffs and the Sub-Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

339. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

340. Therefore, Plaintiffs and the Sub-Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT VI
VIOLATION OF CALIFORNIA'S CONSUMER PRIVACY ACT ("CCPA")
Cal. Bus. Code § 1798.150
(On Behalf of Plaintiffs Morales, Lopez, Marino, and the California Sub-Class Members)

341. Plaintiffs Morales, Lopez, and Marino, individually and on behalf of the California Sub-class, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

342. Defendant violated § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information it voluntarily took responsibility for, and to protect the nonencrypted Private Information of Plaintiffs and the California Sub-class. As a direct and proximate result, Plaintiffs Morales, Lopez, Marino, and the California Sub-class's PII was subject to unauthorized access and exfiltration, theft, or disclosure.

343. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, which collects the personal information of its employees and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

344. Plaintiffs Morales, Lopez, Marino, and California Sub-class members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Private Information, including Plaintiffs Morales, Lopez, Marino, and California Sub-Class members' Private

Information. Plaintiffs Morales, Lopez, Marino, and California Sub-class members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

345. Pursuant to California Civil Code § 1798.150(b), Plaintiffs Marino, Lopez, and Morales mailed CCPA notice letters to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure the deficiencies described within 30 days—and Plaintiffs Morales, Lopez, Marino believe such cure is not possible under these facts and circumstances—then Plaintiffs Morales, Lopez, Marino intend to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

346. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information for which it took responsibility so as to protect that personal information under the CCPA.

347. A judicial determination of this issue is necessary and appropriate at this time to prevent further data breaches by Defendant.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b) For a declaration of rights regarding the reasonable protection of Plaintiffs' Private Information that remains in Defendant's possession and maintenance;

c) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information;

d) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

e) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

f) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

g) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: May 30, 2023

Respectfully Submitted,

/s/ Bryan L. Bleichner

Bryan L. Bleichner (MN #0326689)
Philip J. Krzeski (MN #0403291)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Brian C. Gudmundson (MN #0336695)
Michael J. Laird (MN #0398436)
Rachel K. Tack (MN #0399529)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Phone: (612) 341-0400
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Interim Co-Lead Counsel

Nathan D. Prosser (MN #0329745)
Anne T. Regan (MN #0333852)
HELLMUTH & JOHNSON PLLC
8050 West 78th Street
Edina, MN 55439

Phone: (952) 746-2124
nprosser@hjlawfirm.com
aregan@hjlawfirm.com

Chair of the Executive Committee

Joseph M. Lyon*
THE LYON LAW FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Danielle L. Perry*
Gary E. Mason*
Lisa A. White*
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Phone: (202) 429-2290
dperry@masonllp.com
gmason@masonllp.com
lwhite@masonllp.com

Dylan J. Gould*
Terry R. Coates*
MARKOVITS STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
dgould@msdlegal.com
tcoates@msdlegal.com

David A. Goodwin (MN #0386715)
Daniel E. Gustafson (MN #0202241)
Joe E. Nelson (MN #0402378)
GUSTAFSON GLUEK PLLC
120 South Sixth Street, Suite 2600
Minneapolis, MN 55402
Phone: (612) 333-8844

dgoodwin@gustafsongluek.com
dgustafson@gustafsongluek.com
Jnelson@gustafsongluek.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

John G. Emerson*
EMERSON FIRM, PLLC
2500 Wilcrest Drive, Suite 300
Houston, TX 77042-2754
Phone: (800) 51-8649
Fax: (501) 286-4659
jemerson@emersonfirm.com

Barton D. Cohen*
BAILEY & GLASSER LLP
1622 Locust St.
Philadelphia, PA 19103
Phone: (267) 973-4855
bcohen@baileyglasser.com

Karen Hanson Riebel
Kate M. Baxter-Kauf
LOCKRIDGE GRINDAL NAUEN, P.L.L.P.
100 Washington Ave. South, Ste. 2200
Minneapolis, MN 55401
Phone: (612) 339-6900
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

John A. Yanchunis*
Marco W. Valladares*
Ra. O. Amen*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin St. 7th Floor

Tampa, Florida 33602
Phone: (813) 223-5505
Fax: (813) 223-5402

Kenneth J. Grunfeld*
Kevin W. Fay*
GOLOMB SPIRT GRUNFELD P.C.
1835 Market St., Ste. 2900
Philadelphia, PA 19103
Phone: (215) 346-7338
Facsimile: (215) 985-4169
kgrunfeld@golomblegal.com
kfay@golomblegal.com

Executive Committee Counsel for Plaintiffs and the Putative Class

**Admitted pro hac vice*